Can you hear me?

Current Goal: Quadratic Reciprocity.

Theorem has to do with which elements of $\mathbb{Z}/n\mathbb{Z}$ have a square root.

Example: In $\mathbb{Z}/7\mathbb{Z}$.

a	0	1	2	3	4	5	6
a^2	0	1	4	2	2	4	1

Find that 1, 2, 4 each have two distinct square roots mod 7.

On the other hand, 3, 5, 6 <u>do not</u> have any square roots mod 7.

Convenient notation: Given $a, p \in \mathbb{Z}$ with p prime, define the "Legendre symbol":

$$\left(\frac{a}{p}\right) := \begin{cases} +1 & a \text{ square mod } p \\ -1 & a \text{ non-square mod } p \\ 0 & a \equiv 0 \text{ mod } p \end{cases}$$

Quadratic Reciprocity:

For odd primes p, q we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

This fact leads to an algorithm to compute Legendre symbols.

Example: (Stillwell pg. 171)

$$\left(\frac{37}{59}\right) = +\left(\frac{59}{37}\right) \qquad \text{Q.R.}$$

$$= \left(\frac{22}{37}\right) \qquad \text{remainder}$$

$$= \left(\frac{2}{37}\right)\left(\frac{11}{37}\right) \qquad \text{special case}$$

$$= (-1)\left(\frac{11}{37}\right)$$

$$= (-1)\left(\frac{37}{11}\right) \qquad \text{Q.R.}$$

$$= -\left(\frac{4}{11}\right)$$

$$= -\left(\frac{2}{11}\right)^2$$

$$= -1 \; .$$

Conclusion: 37 is NOT square mod 59.

" There is no easy proof of Q.R.

See: <u>Mathologer video on YouTube</u>

To prepare we will develop some Lemmas.

First: $n = \sum_{d \mid n} \phi(d)$.

Example: 1, 2, 3, 4, 6, 12

$$\cancel{\phi(1)} + \cancel{\phi(2)} + \cancel{\phi(3)} + \phi(4) + \phi(6) + \phi(12) = 12$$

$$\begin{array}{cccccc} 1 & 1 & 2 & \underset{2}{\cancel{2^2-2^1}} & \underset{2}{\phi(2)\phi(3)} & 4 \end{array} \quad \checkmark$$

$$\phi(12) = \phi(2^2)\,\phi(3)$$
$$= (2^2-2^1)(3-1) = 2\cdot 2 = 4$$

Proof: $F_n = \{\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}\}$

$F_n' = \{\frac{k}{n} : \gcd(k,n)=1\} \subseteq F_n$.

Claim: $F_n = \coprod_{d|n} F_d'$ $\quad \subseteq \quad \supseteq$ disjoint.

Hence $n = \sum_{d|n} \phi(d)$.

- $F_n \subseteq \bigcup F_d'$

Given $\frac{k}{n} \in F_n$. Let $\lambda = \gcd(k,n)$

$k = \lambda k'$, $n = \lambda n'$

$\gcd(k', n') = 1$

$n' \mid n$.

Then $\frac{k}{n} = \frac{\lambda k'}{\lambda n'} = \frac{k'}{n'} \in F_{n'}'$ ✓

- $\bigcup F_d' \subseteq F_n$

Consider $\frac{k}{d} \in F_d'$ for some $d | n$, $n = \lambda d$.

Then $\frac{k}{d} = \frac{\lambda k}{\lambda d} = \frac{\lambda k}{n}$ ✓ $\left(\begin{matrix} k \le d \\ \lambda k \le \lambda d = n \end{matrix}\right)$

- $F_d' \cap F_e' \neq \emptyset \Rightarrow d = e.$

Suppose $\alpha \in F_d' \cap F_e'$,

so $\alpha = \underbrace{\frac{k}{d} = \frac{l}{e}}$ where $\gcd(k,d) = 1$, $\gcd(l,e) = 1$

$dl = ek$

$d \mid ek \wedge \gcd(k,d) = 1 \Rightarrow d \mid e.$

$e \mid dl \wedge \gcd(l,e) = 1 \Rightarrow e \mid d.$

$\Rightarrow d = \pm e.$

$\Rightarrow d = e$ (both positive) ✓

Need Another "Lemma": <u>p prime</u>

Any polynomial of degree d & with integer coefficients has $\le d$ roots in $\mathbb{Z}/p\mathbb{Z}$.

Note: primality is necessary!

$x^2 - 1$ has 4 roots $\boxed{\text{mod } 8}$

Namely, $x = 1, 3, 5, 7$ 8 not prime

$4 > 2$!

Key fact: $(\mathbb{Z}/p\mathbb{Z}, +, \cdot, 0, 1)$ is a FIELD, for p prime.

We will prove the more general result:

Let $\mathbb{F}$ be a field.
Any polynomial of degree d with coefficients in $\mathbb{F}$ has $\leq d$ roots in $\mathbb{F}$.

This actually goes back to Descartes' Géométrie (1637)

In modern terms: for any ring R we can define a ring $R[x]$ of "polynomials in x with coefficients from R"

$R[x] = \{ a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots :$
$a_i \in R$, only finitely many are nonzero $\}$

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$
If a_n is the highest nonzero coefficient then we say $\deg(f) = n$.

Given $f(x) = \sum a_i x^i$
$g(x) = \sum b_i x^i$

we define

$$f(x) + g(x) = \sum (a_i + b_i) x^i$$

$$f(x) g(x) = \sum_k \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

Claim: $R[x]$ is a ring.

zero element: $0 + 0x + 0x^2 + 0x^3 + \cdots$
one element: $1 + 0x + 0x^2 + 0x^3 + \cdots$

Convention: For any $a \in R$, we write

$$a + 0x + 0x^2 + 0x^3 + \cdots = a$$

We can think of $R \subseteq R[x]$ as the subring of "constant polynomials"

The ring $R[x]$ can be complicated but if $R = \mathbb{F}$ is a field then the ring is very nice.

$$\mathbb{Z} \qquad\qquad \mathbb{F}[x]$$

share many properties in common.

In particular, the ring $\mathbb{F}[x]$ has "division with remainder".

<u>Theorem</u>: Given $f(x), g(x) \in \mathbb{F}[x]$ where $g(x) \neq 0$, there exist (unique) $q(x), r(x) \in \mathbb{F}[x]$ such that

$$\begin{cases} f(x) = q(x)g(x) + r(x) \\ \deg(r) < \deg(g) \end{cases}.$$

Question: $\deg(0) = \deg(0 + 0x + 0x^2 + \cdots)$

Two options:

- say $\deg(0)$ does not exist.
- say $\deg(0) = -\infty$ for convenience.

Technically:

$$\begin{cases} f(x) = q(x)g(x) + r(x) \\ \underline{\underline{r(x) = 0}} \text{ or } \deg(r) < \deg(g) \end{cases}.$$

The proof is really just an algorithm.

Example: Divide $f(x) = x^3 - 2x^2 + x + 3$

by $g(x) = x - 1$.

$$\begin{array}{r|l}
 & x^2 - x \\ \hline
x - 1 & x^3 - 2x^2 + x + 3 \\
 & \underline{x^3 - x^2 + 0 + 0} \\
 & 0 - x^2 + x + 3 \\
 & \quad \underline{-x^2 + x + 0} \\
 & \qquad\qquad 3
\end{array}$$

Summary: $q(x) = x^2 - x$
$r(x) = 3$

$f(x) = q(x)\, g(x) + r(x)$

$x^3 - 2x^2 + x + 3 = (x^2 - x)(x - 1) + 3$

Remainder is small: $\boxed{x^0 = 1}$

$\deg(3x^0) < \deg(x^1 - 1)$
?
$0 < 1$ ✓

In general, given $f(x) \in \mathbb{F}[x]$
$a \in \mathbb{F}$

we can divide $f(x)$ by $x - a$ to obtain

$$\begin{cases} f(x) = q(x)(x-a) + r(x) \\ \deg(r) < \underbrace{\deg(x-a)}_{1} \end{cases}$$

Hence $r(x) = 0$ or $\deg(r) = 0$

Either way $r(x) = c$ is just a constant polynomial.

Remainder of $f(x)$ mod $x-a$ is a <u>constant</u>. What is the value of the constant?

Check: $f(x) = q(x)(x-a) + c$

Plug in $x = a$:

$$f(a) = q(a)\cancel{(a-a)} + c$$
$$= q(a) \cdot 0 + c = c$$

$$\boxed{c = f(a)}$$

Remainder mod $x-a$ = Evaluation at $x=a$

Descartes' Theorem: Given $f(x) \in \mathbb{F}[x]$ and $a \in \mathbb{F}$, we have

$f(a) = 0$ in $\mathbb{F}$ $\iff$ $f(x)$ divisible by $x-a$ in $\mathbb{F}[x]$.

Corollary: Polynomial $f(x) \in \mathbb{F}[x]$ of degree n has $\leq n$ roots in $\mathbb{F}$.

Proof (Induction on n).

If $f(x)$ has no roots in $\mathbb{F}$, done ✓

Suppose $f(a) = 0$ for some $a \in \mathbb{F}$.

Then Descartes

$\Rightarrow$ $f(x) = g(x)(x-a)$

for some $g(x) \in \mathbb{F}[x]$, $\deg(g) = n-1$.

By induction, $g(x)$ has $\leq n-1$ roots in $\mathbb{F}$.

But if $\underline{f(b)=0}$ for some $\underline{b \neq a}$, then

$$f(b) = g(b)(b-a)$$

$$0 = g(b)(b-a) \qquad b-a \neq 0$$

$$\underline{0 = g(b)}.$$

Hence f has $\leq 1 + (n-1)$ roots in $\mathbb{F}$ ✓